DEPARTMENT OF THE NAVY
NAVY RECRUITING COMMAND
5722 INTEGRITY DR.
MILLINGTON, TN 38054-5057

COMNAVCRUITCOMINST 5239.3
N6
11 Sep 2009

COMNAVCRUITCOM INSTRUCTION 5239.3

From: Commander, Navy Recruiting Command

Subj: NAVY RECRUITING COMMAND INFORMATION SYSTEMS ACCEPTABLE USE POLICY

Ref: (a) COMNAVCRUITCOMINST 5239.1

Encl: (1) Commonly Used Abbreviations

1. Purpose. To establish policy for the governance and use of the Navy Recruiting Command (NAVCRUITCOM) unclassified Wide Area Network (WAN), Navy and Marine Corps Intranet (NMCI) Information Systems (IS), and Information Technology (IT) resources, products, and services. This Acceptable Use Policy (AUP) is designed to protect our customers, the Internet Community, and the Global Information Grid (GIG) from irresponsible, abusive, or illegal activities.

2. Overview. The AUP is not intended to impose restrictions contrary to NAVCRUITCOM's established culture of trust and integrity. NAVCRUITCOM is committed to protecting employees, the command and the GIG from illegal or damaging actions by individuals, either knowingly or unknowingly.

a. NAVCRUITCOM Internet/Intranet/Extranet-related systems (including, but not limited to: computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP) will only be used for business purposes to serve the command staff, field personnel, and customers in the course of normal operations.

b. Effective IS security is a team effort involving the participation and support of every NAVCRUITCOM employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to follow these guidelines, and conduct their activities accordingly.

3. Purpose. To define the acceptable use of NAVCRUITCOM computer equipment and IT resources and protect the command and employees. Inappropriate IT use exposes NAVCRUITCOM to risks including: virus attacks, compromise of network systems and services, and legal liability.

4. Scope. This policy applies to all government issued IT equipment owned or leased by Navy Recruiting Command, military members, government employees, contractors, consultants, temporary employees, and other workers at NAVCRUITCOM, including all personnel affiliated with third parties.

5. Policy

a. General Use and Ownership

(1) While NAVCRUITCOM's WAN provides limited access to appropriate information, users should assume no expectation of privacy. Information contained on NAVCRUITCOM resources is the property of the U.S. Government.

(2) Employees are responsible for exercising good judgment regarding personal use. Individual departments will create guidelines concerning personal use of Internet/Intranet/Extranet systems. Employees should consult supervisors or managers for clarification of departmental guidelines.

(3) Any sensitive or vulnerable information, such as Personally Identifiable Information (PII), should be encrypted using approved encryption methods. For assistance, contact the NAVCRUITCOM Information Assurance Manager (IAM).

(4) For security and network maintenance purposes, authorized individuals within NAVCRUITCOM may monitor equipment, systems, and network traffic at any time, per NAVSO P-5239-08.

(5) NAVCRUITCOM reserves the right to audit networks and systems on a periodic basis to ensure compliance.

b. Protection of Sensitive Information

(1) The user interface (computer) for information contained on Internet/Intranet/Extranet-related systems should be classified as "Sensitive Unclassified." Employees must take

all necessary steps to prevent unauthorized access to sensitive information.

(2) Authorized users are responsible for the security of their passwords and accounts. Keep passwords secure and do not share accounts. System level passwords will be changed monthly and be a minimum of 15 characters long. User level passwords will be changed every 60 days, be a minimum of 14 characters, and utilize the strong password requirements of two uppercase letters, two lowercase letters, two numbers, and two special characters.

(3) Because information contained on portable computers is especially vulnerable, special care must be exercised. For field personnel, after normal business hours, laptop computers will be stored in a locked container (preferably a safe or file cabinet). All personnel traveling or carrying a laptop computer outside a government facility will maintain positive control at all times. If traveling in a vehicle, store the laptop in the vehicle trunk during stops.

(4) Postings by employees from a NAVCRUITCOM email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of NAVCRUITCOM, unless posting is preapproved by the appropriate authority and in the course of official duty.

(5) All hosts used by the employee connected to the NAVCRUITCOM Internet/Intranet/Extranet, whether owned by the command of other DoD entity, will continually execute approved virus-scanning software with a current virus database, unless overridden by Navy or command policy.

(6) Employees will use extreme caution when opening email attachments received from unknown senders. These may contain viruses, email bombs, or Trojan horse codes.

c. Unacceptable Use

(1) Under no circumstances are NAVCRUITCOM personnel authorized to engage in any illegal activity under local, state, federal, or international law while utilizing NAVCRUITCOM-owned resources.

(2) The following activities are strictly prohibited, with no exceptions. The list of activities below is not exhaustive, but attempts to provide a framework for activities which fall into the category of unacceptable use.

(a) Violations of the rights of any person or organization's trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by NAVCRUITCOM.

(b) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which NAVCRUITCOM or the end user does not have an active license is strictly prohibited.

(c) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate NAVCRUITCOM authority should be consulted prior to exporting any material that is in question.

(d) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan Horses, email bombs, etc.).

(e) Revealing your account password, Common Access Card Personal Identification Number (CAC PIN), or allowing use of your account by employees. This includes family and other household members when employees work at home.

(f) Using a NAVCRUITCOM computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

(g) Making fraudulent offers of products, items, or services originating from any NAVCRUITCOM account.

(h) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to: network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

(i) Port scanning or security scanning is expressly prohibited unless prior notification to NAVCRUITCOM is made.

(j) Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

(k) Circumventing user authentication, the security of any host, network, or account.

(l) Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

(m) Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session; via any means, locally or via the Internet/Intranet/Extranet.

(n) Providing information about, or lists of, NAVCRUITCOM employees to parties outside NAVCRUITCOM.

(o) Copying of PII or Privacy Act (PA) material onto personally owned computing device.

d. Email and Communications Activities

(1) Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

(2) Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

(3) Unauthorized use, or forging of email header information.

(4) Solicitation of email for any email address (other than that of the poster's account) with the intent to harass or collect replies.

(5) Creating or forwarding "chain letters", "Ponzi" or "pyramid" schemes of any type.

(6) Use of unsolicited email originating from within NAVCRUITCOM's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by NAVCRUITCOM or connected via NAVCRUITCOM's network.

(7) Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

e. Blogging

(1) Blogging by employees, whether using NAVCRUITCOM’s property and systems or personal computer systems, is also subject to the terms and restrictions per this policy. Limited and occasional use of NAVCRUITCOM’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate policy, is not detrimental to Navy interests, and does not interfere with an employee's regular work duties. Blogging from NAVCRUITCOM systems is subject to monitoring.

(2) Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of NAVCRUITCOM and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory, or harassing comments when blogging or otherwise engaging in any conduct prohibited by the Navy’s or NAVCRUITCOM’s Non-Discrimination and Anti-Harassment policy.

(3) Employees may not attribute personal statements, opinions, or beliefs to NAVCRUITCOM when engaged in blogging. If an employee is expressing personal beliefs and/or opinions in blogs, they may not, expressly or implicitly, represent themselves as an employee or representative of NAVCRUITCOM. The employee assumes any and all risk associated with blogging.

(4) Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, NAVCRUITCOM’s trademarks, logos and any other intellectual property may not be used in connection with any blogging activity.

6. Enforcement. Any employee or service member found to have violated this policy will be subject to disciplinary action. Disciplinary action may include, but is not limited to: temporary revocation of access to Navy and NAVCRUITCOM IT resources, formal/informal counseling, termination, NJP, and/or courts-martial.

/s/
R. R. BRAUN

Distribution:
Electronic only, via
http://www.cnrc.navy.mil/Publications/directives.htm

Commonly Used Definitions

Term Definition

Blogging Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.

Email Bomb A form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.

Extranet A private network that uses Internet Protocols, network connectivity, and the public telecommunications system to securely share part of an organization's information or operations with suppliers, vendors, partners, customers or other businesses.

FTP A standard network protocol used to exchange and manipulated files over an Internet Protocol computer network, such as the Internet.

Internet A global system of interconnected computer networks that use the standardized Internet Protocol Suite (TCP/IP) The internet consists of millions of private and public, academic, business, and government networks of local to global scope that are linked by copper wires, fiber optic cables, wireless connections, and other technologies.

Intranet A private computer network that uses Internet technologies to securely share any part of an organization's information or operational systems with its employees. Sometimes the term refers only to the organization's internal website, but often it is a more extensive part of the organization's information technology infrastructure and private websites are an important component and focal point of internal communication and collaboration.

Pinged Flood A simple denial-of-service attack where the attacker overwhelms the victim with Internet Control Message Protocol ICMP Echo Request (ping) packets.

Term Definition

Piracy Or ***copyright violation,*** The unauthorized use of material that is covered by copyright law, in a manner that violates one of the copyright owner's exclusive rights, such as the right to reproduce or perform the copyrighted work, or to make derivative works.

Ponzi Scheme A fraudulent investment operation that pays returns to separate investors from their own money or money paid by subsequent investors, rather than from any actual profit earned.

Pyramid Scheme A non-sustainable business model involving the exchange of money primarily for enrolling other people into the scheme, often without any product or service being delivered.

Spoofing A situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Sniffing Computer software or computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and eventually decodes and analyzes its content according to the appropriate Request For Comment (RFC) or other specifications.

Spam Unauthorized and/or unsolicited electronic mass mailings.

Trojan Horse A term used to describe malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system. Trojan horses are not self-replicating which distinguishes them from viruses and worms. Additionally, they require interaction with a hacker to fulfill their purpose.

Virus A computer program that can copy itself and infect a computer without the permission or knowledge of the owner. A virus can only spread from one computer to another when its host is taken to the target computer; via a removable medium such as a floppy disk, CD, DVD, or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer.

Term Definition

Worm A self-replicating computer program. It uses a network to send copies of itself to other computers on the network and it may do so without any user intervention. Worms almost always cause at least some harm to the network, if only by consuming bandwidth.

Usenet A worldwide distributed Internet discussion system.